Evaluation of Time Sensitive Networks (TSN) for Use in Army Aviation Platforms

Brijesh Patel
PeopleTec, Inc.
Huntsville, AL
Brijesh.Patel@peopletec.com

Jimmy Moore
PeopleTec, Inc.
Huntsville, AL
Jimmy.Moore@peopletec.com

Brett Boren
Redstone Test Center
Redstone Arsenal, AL
brett.a.boren.civ@army.mil

Jonathan Hardy
IronMountain Solutions
Huntsville, AL
jonathan.hardy@imsinc.us

ABSTRACT

The US Army Program Executive Office for Aviation (PEO AVN) is preparing for future avionics migration from legacy data distribution interfaces (MIL-STD-1553, ARINC 429) to Ethernet-based communications. This transition is foundational to PEO AVNs digital backbone concept and offers benefits such as high bandwidth, increases reliability by minimizing packet loss or dropout, network synchronization, and increased security. PEO AVN is addressing this transition by implementing time sensitive networks (TSNs) based on the Institute of Electrical and Electronics Engineers (IEEE) 802.1 standards. These standards support real-time, deterministic communication which is essential for flight critical systems.

However, this evolution presents several challenges. Notably, the current test and evaluation (T&E) infrastructure required to evaluate effectiveness, flight safety, airworthiness, adherence to modular open systems approach (MOSA) objectives, cybersecurity, and integration with legacy mission equipment is lacking.

This paper presents a Modeling and Simulation (M&S) environment for T&E of TSN systems. Utilizing a simulated UH-60M Cockpit with visual, avionics, and flight control systems, we generate simulated vehicle state data and model line replaceable unit (LRU) input/output (I/O) signals in legacy formats to study and address interface issues with TSN based communications. The environment facilitates the development of instrumentation and tests the integration of LRUs with both TSN-native and legacy interfaces over the TSN network. Additionally, the team is developing custom Ethernet network analyzer tools to assess key network performance metrics such as jitter, latency, bandwidth, and key network performance metrics across various scenarios. This enables PEO AVN to reduce risk for digital backbone designs and provides comprehensive evaluation of TSN networks, validating architecture integration, MOSA compliance, and network performance, while optimizing TSN solutions for time-sensitive applications.

ABOUT THE AUTHORS

Brijesh Patel is a Technical Lead in M&S at PeopleTec, Inc., where he leads the development of hardware-in-the-loop (HWIL) test environments for Redstone Test Center (RTC) focused on T&E of TSN systems by leading the software architecture effort for simulated avionics, and the development of analysis tools to validate TSN Quality of Service. Brijesh holds a Master of Science in Aerospace Systems Engineering and a Bachelor of Science in Mechanical Engineering, both from the University of Alabama in Huntsville. His prior experience spans computational analysis, radar systems modeling, and software development for defense applications.

Jimmy Moore is a Senior Technical Fellow for PeopleTec, Inc. supporting Program Manager Future Long Range Assault Aircraft (PM FLRAA) as a M&S subject matter expert (SME). He is a Certified Modeling and Simulation Professional (CMSP) with over 30 years of experience in M&S supporting design, development, fielding, and modifications of aircraft and missile systems utilizing distributed, man-in-the-loop, and training applications. Experience includes crew station working group (CSWG) M&S support for human factors, development of training aids, devices, simulations and simulators (TADSS) for Army Aviation (UH-60, CH-47); synthetic environments for manned and HWIL simulations, and support to science, technology, engineering and math programs to include design and development of distributed simulation exercises.

Brett Boren is the M&S SME for RTC at Redstone Arsenal, AL. He has more than 20 years of experience building and operating missile HWIL labs and aviation installed system test facilities for systems such as the AGM-148 Javelin, the AGM-114L HELLFIRE Longbow, the AN/AAR-57 Common Missile Warning System and similar systems. He has also led Live, Virtual, Constructive (LVC) simulations leveraging distributed test and simulation technologies both within the DoD and with international partners and has taught LVC Integrated Process classes at the Interservice/Industry Training, Simulation and Education Conference (I/ITSEC) and for DoD and industry partners.

Jonathan Hardy is a Director for IronMountain Solutions, LLC supporting PM FLRAA as an architecture, software, and cybersecurity SME. He is a network engineer with a bachelor's degree in information systems; a master's in business administration with a focus on project management with 10 years' experience in exploiting and securing DoD tactical weapon systems. He holds several certifications to include being a Certified Information Systems Security Professional (CISSP). He has 20 years' experience in cybersecurity where he started in cyber intelligence specialist for the United States Marines with tactical experience gained during Operation Iraqi Freedom (OIF) I, II, and the Horn of Africa from 2002-2007. Following his service, he worked as a flight test engineer for RTC where he focused on software and cyber to include exploitation of real time operating systems (RTOS), ARINC 429, MIL-STD-1553, and other standards such as automatic dependent surveillance–broadcast (ADS-B). Following his work as flight test engineer, he was a cybersecurity SME for the Apache Program Management Office (PMO) where he was instrumental in the development of the test strategy for the National Defense Authorization Act (NDAA) 1647 Assistant Secretary of the Army (ASA) for Acquisition, Logistics, and Technology (ALT) assessments for the top 50 Department of Defense (DoD) weapon systems.

Evaluation of Time Sensitive Networks (TSN) for Use in Army Aviation Platforms

Brijesh Patel
PeopleTec, Inc.
Huntsville, AL
Brijesh.Patel@peopletec.com

Jimmy Moore
PeopleTec, Inc.
Huntsville, AL
Jimmy.Moore@peopletec.com

Brett Boren
Redstone Test Center
Redstone Arsenal, AL
brett.a.boren.civ@army.mil

Jonathan Hardy
IronMountain Solutions
Huntsville, AL
jonathan.hardy@imsinc.us

Introduction and Background

The US Army's Program Executive Office for Aviation (PEO AVN) is migrating from legacy data distribution interfaces (i.e., MIL-STD-1553, ARINC 429) to ethernet-based communications to leverage higher bandwidth, improved reliability, network synchronization, and enhanced security. PEO AVN is implementing the Institute of Electrical and Electronics Engineers (IEEE) 802.1DP – Time Sensitive Network (TSN) for Aerospace Onboard Ethernet Communications standard to enable deterministic, low latency, highly reliable and synchronized communication essential for flight-critical and mission-critical systems.

For decades, military aviation platforms have relied on standards like MIL-STD-1553 and ARINC 429, which are known for their reliability, fault tolerance, and deterministic communication protocols. MIL-STD-1553, introduced in 1973 with a data rate of 1 Mbps (Data Device Corporation [DDC], 2016). While MIL-STD-1553C, released in 2018, remains the official DoD standard, Enhanced Bit Rate 1553 (EBR-1553) and HyPer-1553 offer increased data throughput (10 Mbps and ~200 Mbps respectively) while maintaining compatibility with 1553 cabling and signaling schemes (Data Device Corporation [DDC], 2016). However, neither EBR-1553 nor HyPer-1553 are formally recognized military standards under the MIL-STD-1553 series. These initiatives are vendor-specific solutions to meet program-specific requirements, and while they may be used in government or aerospace applications, they do not carry formal MIL-STD designation. ARINC 429, a unidirectional, point-to-point protocol transmitting 32-bit words at 12.5 or 100 kbps, is widely used in commercial and military aircraft due to its simplicity and reliability. Yet, it is limited by the number of messages that can be transmitted over a single connection, lacks scalability, multi-node flexibility, and dynamic addressing—factors essential for integrating modern avionics functions (Janiczek, 2021). The aerospace industry has also implemented other standards to meet bandwidth requirements and leverage new technologies (i.e. fiber optic cabling), including IEEE 1394 (Firewire), ARINC 629 (Serial), MIL-STD-1760 (Fiber), ARINC 825 (Controller Area Network [CAN]), ARINC 664 Part 7 (Avionics full-duplex switched Ethernet (AFDX)), SAE AS6802 (Time Triggered Ethernet (TTE)), and TSN IEEE 802.3 (Ethernet) (Jabbar, 2024).

The Army's Migration to TSN

To meet modern aviation system requirements (scalability, performance, reliability, open systems architecture, cybersecurity, and sustainability), PEO AVN defined the acceptable/required protocols for the data distribution service (DDS) for digital backbone (DBB) implementation. Several vendors selected and implemented TSN to meet this requirement. The IEEE P802.1DP TSN profile builds upon existing Ethernet standards, integrating a curated set of enhancements and modifications—such as those defined in IEEE 802.1AS Timing and Synchronization Protocol, 802.1Qbv Ethernet Time-Aware Shaper (TAS), and 802.1CB Frame Replication and Filtering for Reliable Industrial Networks and others—to make Ethernet communication deterministic and suitable for critical aerospace applications. Rather than reinventing Ethernet, the profile standardizes a subset of existing TSN features while defining specific configuration parameters, ensuring LRU interoperability, real-time performance, and reliability for onboard networks in aircraft (IEEE 802.1, 2021).

Since 2012, the IEEE TSN task group has been working to standardize real-time Ethernet capabilities and research efforts have increased to determine the viability of replacing buses like MIL-STD-1553 and ARINC 429 in commercial aviation (Seol, 2021). AFDX (ARINC 664 Part 7) adopted by commercial aviation provides deterministic communication through virtual links (VLs) and bandwidth allocation gap (BAG)-based scheduling, offering bounded latency and jitter (Tyagi, 2017). However, AFDX has key limitations: 1) it lacks native time synchronization, 2) is statically configured, 3) it is semi bandwidth limited, 4) is semi-proprietary, and 5) depends on proprietary hardware These factors restrict scalability, adaptability, and especially challenge military applications that require dynamic reconfiguration, robust timing, and commercial-off-the-shelf (COTS) interoperability. TSN aligns with the Army's goals for modularity, scalability, and mission agility. Army modernization programs like FLRAA, H-60M Black Hawk, and the High Accuracy Detection and Exploitation Systems (HADES) are exploring TSN as a more flexible alternative as it supports the following main features:

- **Precise time sync** via IEEE 802.1AS2020 (gPTP), enabling coordinated communication across devices – unlike AFDX, which lacks native time sync and is less suited for tightly coordinated, high-bandwidth operations (Finzi et. al., 2018).
- **Centralized configuration (**IEEE, 2017) with Centralized Network Configuration (CNC), unlike AFDX's static VLs.
- **Mixed-criticality traffic** using IEEE 802.1Qbv time-aware shaper (TAS), 802.1Qci per-stream filtering and policing (PSFP), and burst limiting shaper (BLS) without sacrificing determinism.
- **Improved performance** with lower latency, higher bandwidth, COTS hardware, and built-in redundancy.

Challenges in Transitioning to TSN

Transitioning to an Ethernet-based TSN backbone introduces new cybersecurity challenges for flight-critical systems. Legacy protocols like MIL-STD-1553 and ARINC 429 were closed and isolated, making them inherently resistant to modern IP network-based threats and often require development of custom exploits. TSN's Ethernet foundation is vulnerable to traditional cybersecurity penetration tools such as spoofing, denial-of-service, and unauthorized access using known pre-develop exploits. To secure avionics data flows without compromising real-time performance, TSN systems must integrate IEEE 802.1 security mechanisms—including 802.1X port authentication and 802.1AE MACsec encryption; however, these protections add latency and complexity and must be carefully evaluated to avoid impacting safety-critical operations. Aviation environments require a fail-open strategy, prioritizing data delivery over containment, which often conflicts with traditional cybersecurity practices. Existing frameworks like the National Institute of Standards and Technology (NIST) risk management framework (RMF) and Radio Technical Commission for Aeronautics (RTCA) DO-326A (Airworthiness Security Process Specification) need adaptation to TSN's unique properties—such as its determinism, strict timing, and ability to detect out-of-plan traffic. Ultimately, cybersecurity for TSN in aviation demands a risk-based approach that balances safety, security, and performance, and supports airworthiness certification through tailored processes and controls.

A key challenge is demonstrating that TSN's complex features (e.g., scheduling, shaping, policing) behave predictably under all conditions. Certifying flight-critical data flows involves verifying bounded latency, jitter, and loss probabilities—a far more complex task than with traditional buses (Castro-Lara et al., 2025). All TSN configurations (along with its hardware, firmware, and software) effectively become part of the aircraft's design baseline requiring validation under safety standards such as ARP 4754A and ARP 4761, especially for new failure modes like time sync loss or traffic shaper misconfiguration. While TSN supports dynamic reconfiguration—a benefit for the Army's MOSA goals—current airworthiness certification processes do not yet accommodate rapid changes for flight-critical flows. Certification will require new artifacts, including validated network configurations, test strategies, and documentation of shaping/scheduling per IEEE 802.1Qbv and Qav. Compliance with DO-178C, DO-254, and DO-330-certified tools will also be essential for qualifying TSN switch software and hardware.

Modern flight test instrumentation captures data like MIL-STD-1553, ARINC 429, Ethernet, video feeds, strain gauges, and other system-specific signals. This data helps engineers evaluate system requirements and performance against verification test criteria; however, TSN significantly increases the volume and complexity of data exchanged across systems—potentially exceeding current instrumentation capabilities. One key challenge is that traditional buses like 1553 and ARINC 429 allow passive data collection by simply adding an endpoint. TSN requires test equipment to either be integrated into the network or act as a delay-free, non-intrusive "man-in-the-middle," complicating the goal of non-disruptive testing. Another challenge is that cybersecurity protections on instrumentation complicate testability. Modern TSN-enabled systems may enforce strict access controls or end-to-end encryption, potentially blocking test instrumentation if not pre-integrated into secure environments. These controls, while critical for

airworthiness, can limit visibility into critical traffic unless key management and access policies are explicitly tailored for test scenarios. This often results in higher costs due to specialized software builds or dedicated test configurations. Additionally, networks implementing IEEE 802.1X or IEEE 802.1AE Media Access Control Security (MACsec) may require test equipment to authenticate as trusted endpoints before capturing or injecting data, which may be infeasible in highly controlled test environments. Further, any deviation from the operational configuration, such as inserting passive taps, could be flagged as a security violation and trigger traffic shutdowns or invalid test results. Test teams must now coordinate closely with cybersecurity and network engineers to ensure instrumentation methods are compliant with system-level protection mechanisms and can still yield trustworthy, complete datasets under secure operating conditions. Finally, timing remains a critical instrumentation concern. TSN's reliance on precise time synchronization across all nodes requires that test systems align perfectly with the aircraft's timing domain. Any drift or offset could lead to misalignment of data streams, invalidating performance assessments. Instrumentation tools must therefore support synchronization protocols like IEEE 802.1AS and include rigorous calibration capabilities (Pop, Craciunas, & Schedel, 2018). Without purpose-built TSN-aware test instrumentation, validating these networks risks becoming a bottleneck in both development and certification efforts.

Developing a Test Environment for TSN Evaluation Utilizing M&S

There is a critical need to develop and sustain, within PEO AVN, a T&E environment to validate TSN-based DDS implemented on Army assets. RTC is addressing this by developing a HWIL M&S environment to test TSN-based DDS architecture across various implementations and aircraft platforms called Mission Systems Test Capability (MSTC). MSTC is a modular setup that utilizes the Cockpit Academics Procedural Tool-Enhanced with Visual and Flight Control System (CAPTE-VCS) to generate air vehicle state data, enabling both simulation of LRU signals and stimulation of actual LRUs integrated with TSN components. The environment is designed not only for the independent verification and validation (IV&V) of TSN architecture, but also for early evaluation activities like toolchain assessments, developmental hardware testing, and identifying integration challenges, particularly those involving legacy signal compatibility within TSN based DDS. The physical layout of the MSTC lab is shown in Figure 1. Key hardware and software elements that form the MSTC environment include the Software Evaluation Station (SWES), Digital Backbone Stimulation Software (DiBS), TSN Analysis Suite, Flight Tracker and Instruments software.

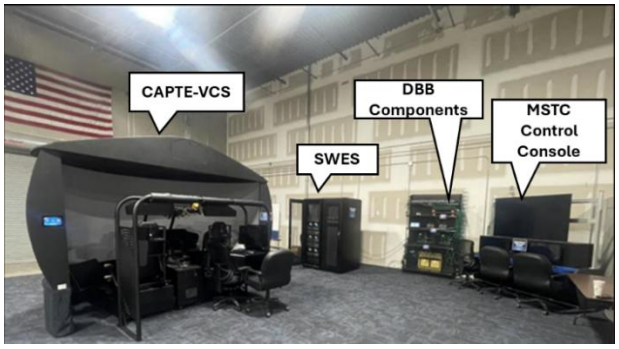

Figure 1: MSTC Lab Layout Including CAPTE-VCS, SWES, and MSTC Console

MSTC Hardware Components

CAPTE-VCS provides a realistic operational environment by simulating a UH-60M Black Hawk cockpit (Figure 1). The simulation utilizes government-off-the-shelf (GOTS) simulated avionics coupled with X-Plane software to generate Out-the-Window (OTW) visual displays. Within MSTC, the CAPTE-VCS is used solely as a source of simulator-driven system state data. This data is converted into I/O signals that emulate LRUs and flow through a TSN architecture to establish a surrogate TSN-based DDS. Since CAPTE-VCS serves solely as a source of system state data, the TSN-based vehicle bus is configured externally. As a result, external physical LRUs cannot currently interface directly with CAPTE-VCS, as it operates as a closed system without bidirectional data flow.

The SWES is a two-rack system that houses workstations, data storage, I/O cards (MIL-STD-1553, ARINC 429 and TSN Network Interface Cards [NICs]), and a Keyboard Video Mouse (KVM) distribution system. The KVM setup enables users to switch between different workstations based on mission requirements. TSN components connect to the SWES via a dedicated management network, which pushes configurations to the respective components.

A MSTC control console provides centralized access and control over multiple test workstations, enabling users to switch seamlessly between up to three systems in real time. Using a KVM system, users can switch between workstations in real time without physically interacting with each one. This streamlined interface supports efficient configuration, monitoring, and execution of test scenarios, reducing setup time and facilitating a cohesive testing workflow across HWIL and TSN environments.

MSTC Software Components

The Flight Tracker and Instruments software displays the state data going through the TSN DDS components as shown in Figure 2. The Flight Tracker uses Cesium with offline imagery to display the flight path and vehicle orientation on a street view map while the Flight Instrument software visually displays real time data on virtual flight instruments.

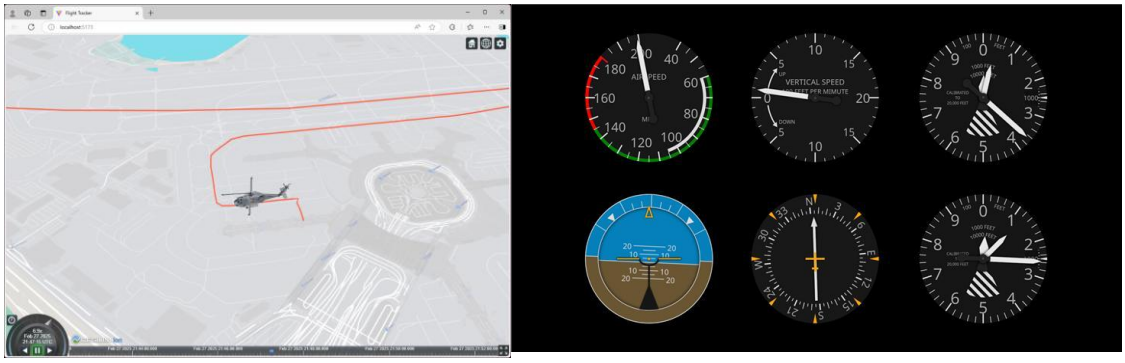

Figure 2: Flight Tracker and Instrumentation Software Views

DiBS has been developed to support dynamic and flexible testing of TSN based Data Distribution Systems. DiBS serves as a critical component for simulating LRUs via I/O signals, stimulating TSN components via randomly generated traffic, and analyzing network traffic across multiple avionics interfaces without requiring code-level changes. DiBS provides the following main capabilities for MSTC:

- Transmitting and receiving vehicle state data from CAPTE-VCS to SWES
- Generating and processing I/O signals using either CAPTE-VCS vehicle state data or randomly generated data. DiBS can support the following three interfaces:
    - User-defined MIL-STD-1553 signals via AltaDt 1553 card
    - User-defined ARINC 429 signals via AltaDt 429 card
    - User-defined Ethernet message in UDP protocol (using TSN capable PCIe NICs)

The TSN Analysis Suite is a comprehensive software suite developed to evaluate and visualize the behavior of TSN traffic in complex avionics environments. Designed to support both development and test phases, the suite enables engineers to monitor, diagnose, and refine TSN configurations for improved performance and reliability.

MSTC Integration

MSTC integrates a wide range of hardware and software components to support TSN and legacy systems. These components enable the emulation, monitoring, configuration, and testing of complex networks and interfaces, ensuring compatibility between modern TSN protocols and legacy systems like MIL-STD-1553 and ARINC 429. The MSTC console includes the following TSN devices:

- **Switch:** Serves as the core TSN switch, forwarding traffic based on schedules and VL configurations.
- **End Point / Bridge:** Functions as a TSN-capable device for generating and receiving traffic; emulates avionics nodes or bridges traffic flows.
- **Programmable End Point / Bridge:** Enables flexible integration and testing of TSN traffic using a configurable, programmable interface.
- **Traffic Recorder / Measurement Tool:** Captures and analyzes TSN traffic in real time to verify latency, jitter, and synchronization across the network.
- **TSN Configuration Software:** Helios supports network design and stream definitions, while Chronos computes the schedule and generates configuration files in YANG/JSON format.
- **Data Concentrator (DC) with TSN Bridge:** A general-purpose computer that converts MIL-STD-1553 and ARINC429 I/O to Ethernet traffic applying TSN Quality of Service (QoS), and vice versa.

The legacy digital cards and LRUs integrated in MSTC are:

- **MIL-STD-1553 I/O Generator:** Emulates MIL-STD-1553 data channels to test legacy communications.
- **ARINC429 I/O Generator:** Emulates ARINC429 data channels to test legacy avionics interfaces.
- **Embedded GPS/INS LRU:** Provides position and navigation data to support system-level testing.

The lab is physically connected as shown below in Figure 3, which illustrates the high-level network connectivity between components. The SWES 1 and SWES 2 racks host elements of the PESA system that provide centralized KVM functionality. The KVM system is essential for enabling MSTC users to seamlessly access and control any of the 10 workstations—five with Linux OS and five with Windows OS—from either the main MSTC console (with three displays) or the Control Room (with six displays). This eliminates the need for physically moving between stations and streamlines testing, monitoring, and control tasks. Equally important is the dedicated management network, which connects all TSN DDS components and the CAPTE-VCS system. This network allows for efficient, centralized configuration, control, and health monitoring from any workstation within SWES 1. By isolating management traffic from real-time test data, the network ensures system stability, security, and performance integrity. Together, the KVM system and management network establish the foundation for the software toolchain.

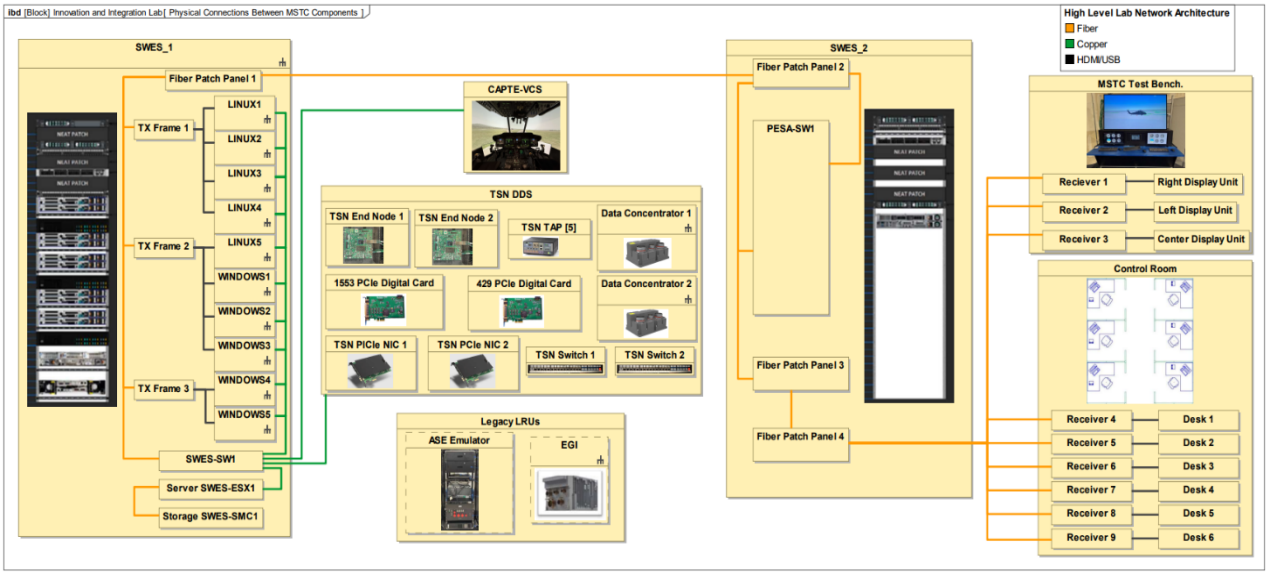

Figure 3: Physical Connections Between MSTC Components

Using MSTC to Generate and Validate TSN Traffic

MSTC users configure TSN devices by specifying all TSN devices, including their tolerances, capabilities, and compatibility with the IEEE 802.1Qcc YANG data model. Users then develop the network topology in Helios and define the stream parameters such as traffic class type, IP addresses of TSN bridges and management ports, and MAC addresses of sender and receiver devices. Once the topology and stream definitions are complete, the project is saved in Helios, generating input files for Chronos containing all defined network and stream information. Finally, from Helios to compute the TSN network's scheduling solution and generates configuration files for each TSN Chronos uses the input device in YANG or JSON formats (Figure 4).

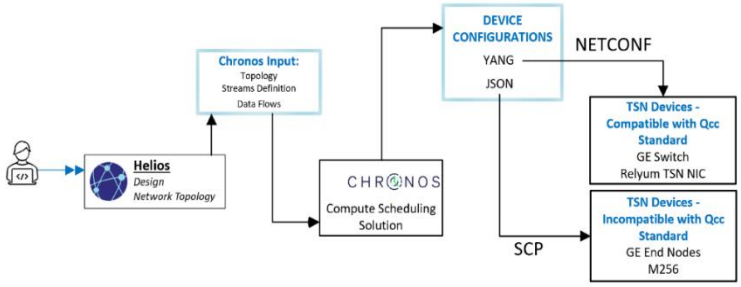

Figure 4: TSN Toolchain Workflow

Methods for Generating TSN Device Traffic

Flight-simulated data from CAPTE-VCS is shared through the host computer, which runs DiBS software to format the data as JSON-formatted UDP packets and send it across the SWES management network. Two workstations equipped with AltaDt PCIe cards receive this data and convert it into MIL-STD-1553 or ARINC 429 messages. These messages are then processed by the DC general purpose computer, which converts them into TSN Ethernet frames with the appropriate QoS. This process is shown in Figure 5.

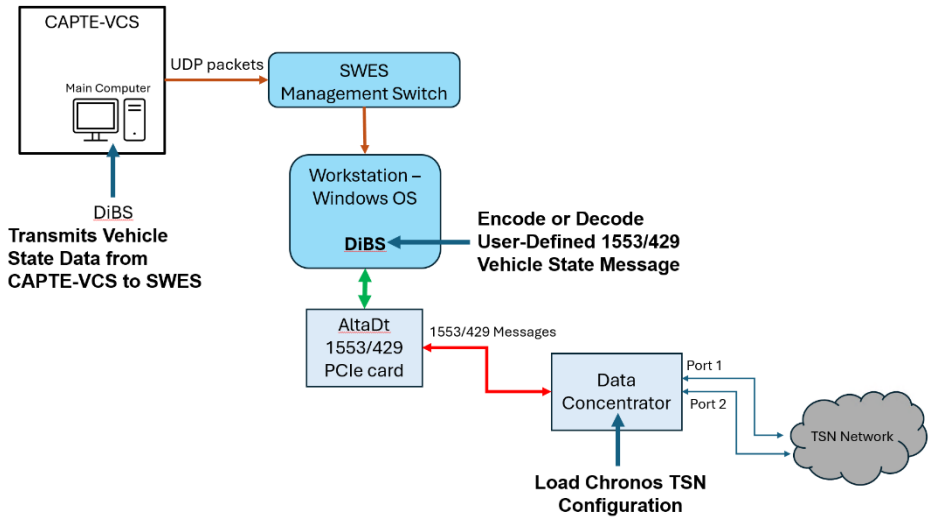

Figure 5: Data Flow from CAPTE-VCS to TSN Network via 1553/429 PCIe Card and Data Concentrator

The specific role of the DC varies depending on the signal type being processed, as outlined below:

- **MIL-STD-1553 Data Flow:** The DC acts as a Bus Controller, receiving messages from the AltaDt PCIe card and converting them into TSN Ethernet traffic.
- **ARINC 429 Data Flow:** The DC receives ARINC 429 messages and translates into TSN Ethernet frames.

Integrating Native TSN Signals Using Simulated Flight Data

Some TSN platforms tightly integrate with configuration toolchains that automatically generate VLAN interfaces. In contrast, general-purpose systems like those running Linux OS require manual VLAN interface creation for each stream (Figure 6). This discrepancy arises because the IEEE 802.1Qcc standard defines centralized configuration through CNC but does not specify how VLAN interface instantiation at the host level.

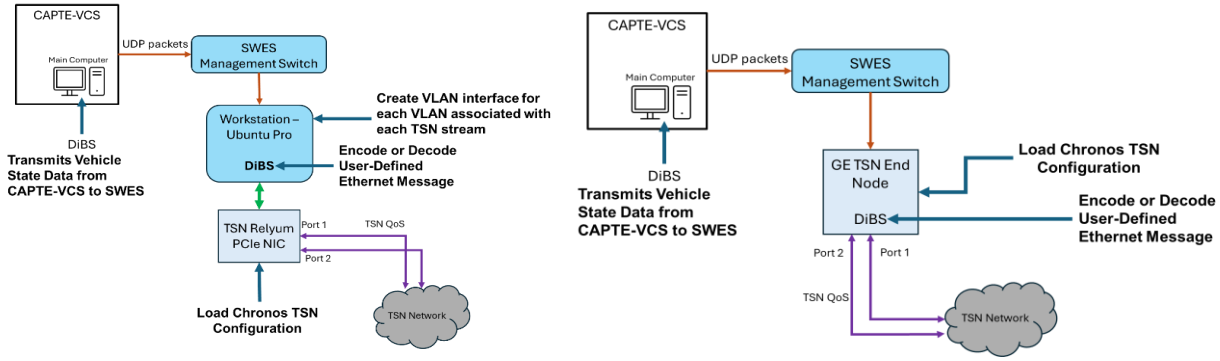

Figure 6: Data Flow from CAPTE-VCS to TSN Network via End Nodes

MSTC Applied TSN Features and Test Configuration for Evaluation

MSTC applied several TSN features defined in the IEEE 802.1DP profile across the test network to evaluate TSN device behavior under realistic conditions. The traffic stream types used include:

- **Scheduled Stream**: Configured using TAS for deterministic delivery of time-critical data.

- **Frame Replication and Elimination for Reliability (FRER)**: Enhances fault tolerance by transmitting duplicate copies of critical frames across disjoint network paths and eliminating duplicates at the receiver.
- **Guaranteed Bandwidth using PSFP**: Ensures each stream adheres to its allocated bandwidth and traffic profiles, maintaining QoS by filtering and policing at ingress, preventing bandwidth overruns.
- **Best Effort**: Allows non-critical data transmission without timing guarantees, using remaining bandwidth after prioritizing scheduled and critical traffic.

MSTC supports sending and receiving MIL-STD-1553, ARINC 429, and Native TSN Signals through TSN architecture. The reconfigurable MSTC lab space can be tailored to meet specific testing objectives. Figure 7 shows a generic TSN topology for validating the IEEE 802.1DP profile features, with Switch 1 designated as the Master Clock.

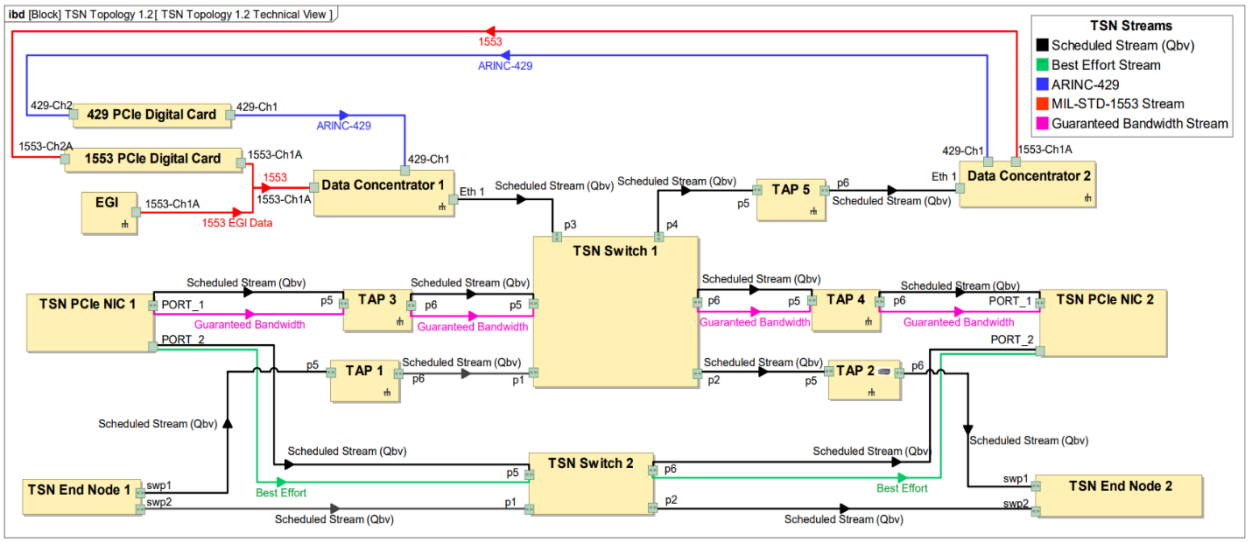

Figure 7: Generic MSTC Topology

The MSTC testbed has been crucial for RTC in validating critical TSN capabilities through extensive testing, monitoring, and analysis. MSTC uses network Test Access Points (TAPs) with hardware that timestamps in accordance with IEEE 802.1AS-2020, synchronizing with the network and recording traffic with a granularity of eight nanoseconds. This precise timestamping supports detailed jitter and latency analysis, enabling comprehensive validation of TSN functionality, including scheduling, policing, and redundancy. TAPs can also inject gPTP synchronization errors for stress-testing TSN timing resilience, while the TSN Analysis Suite provides detailed insights into all unique streams. This approach ensures MSTC can effectively assess system behavior, troubleshoot issues, and evaluate TSN-aware diagnostic strategies in support of safety- and mission-critical applications.

To validate the performance of a scheduled stream, traffic was captured at each hop across the TSN network using network TAPs, allowing analysis of inter-message timing at every switch. The inter-message gap (IMG_i) defined as:

$$IMG_i = t_i - t_{i-1}$$

where t_i and t_{t-1} are the timestamps of two consecutive packets in the stream. Jitter at each hop is calculated as:

$$Jitter = |IMG_i - T_{Schedule}|$$

where $T_{Schedule}$ is expected schedule of the interval of the scheduled stream. The TSN Analysis Suite computes and plots the jitter distribution at each hop, verifying that timing variations remain within allowable tolerances and validating the timing integrity of the scheduled flow. Figure 8 shows an example of a jitter plot for three different streams.

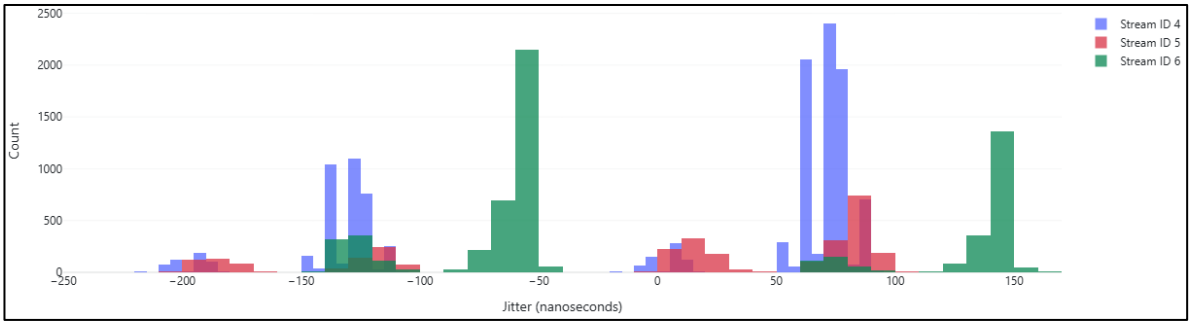

Figure 8: Jitter Plot for Scheduled Stream over a TSN Network

To validate guaranteed bandwidth enforcement, network TAPs at each hop monitor the behavior of policed streams, capturing live traffic and timestamp packets for precise throughput measurements across the network path. Using this data, the TSN Analysis Suite calculates per-hop throughput and identifies discrepancies. If a stream exceeds its allocated bandwidth, drops are traced to the enforcing node, validating that:

- The stream adheres to its configured rate across hops.
- Excess traffic is consistently and predictably dropping.
- No unintended drops occur for in-profile traffic.

For FRER validation, the TSN network uses two redundant paths through separate switches, with TAPs to monitor traffic flow and verify correct replication and elimination behavior. Under normal conditions, both paths carry identical frames, and the receiver accepts only the first valid frame, discarding duplicates. During resilience testing, one switch is powered down or disconnected mid-stream and TAPs confirm that:

- The stream remains uninterrupted from the speaker to the listener.
- The receiver seamlessly continues processing packets from the remaining active path.
- No duplicate or lost frames occur during the failover transition.

For stream isolation, a scheduled stream is transmitted on a dedicated 802.1Qbv time slot while a high-volume flood of non-critical traffic mimics a Denial of Service (DoS) attack on the same link through a separate device targeting the same receiver. TAPs monitor traffic at the ingress and egress points, confirming that:

- The scheduled stream is consistently received without delay or loss.
- The receiver filters or drops all excess traffic outside the scheduled window.
- Network scheduling and prioritization effectively isolate time-critical flows from disruptive traffic.

This test demonstrates TSN's robustness in maintaining deterministic behavior under hostile conditions.

Summary of MSTC Features and Future Enhancements

The MSTC facility supports IV&V of TSN architectures, toolchains, and data flows proving effective in bridging legacy and modern avionics interfaces, supporting deterministic TSN traffic, and reducing integration risk through:

- **Early T&E and Risk Reduction:** Facilitates early evaluation of TSN equipment, software, and integration challenges, reducing risk in avionics system development and certification.
- **Multi-Protocol Interoperability:** Demonstrates end-to-end determinism by routing and converting legacy I/O (MIL-STD-1553, ARINC 429) through TSN infrastructure, maintaining flight system protocol compatibility.
- **TSN Toolchain Functionality:** Assesses Chronos and Helios toolchains and network configurations for defining, scheduling, and deploying TSN streams using the IEEE 802.1Qcc YANG model.
- **Integration Testbed:** Provides a modular environment for integrating legacy and TSN-native systems using simulated mission-relevant data, enabling testing of protocol bridging, stream scheduling, and real-time visualization, revealing compatibility and timing issues and supports dual-path data validation.
- **Manual VLAN Configuration:** The IEEE 802.1DP profile defines CNC via IEEE802.1Qcc but does not specify the generation of VLAN interfaces through the CNC process. As a result, VLANs must be manually configured at the OS/application layer to enable policing of proper traffic classification through IEEE802.1Qci enforcement. This applies to both general purpose and embedded Linux systems, although embedded platforms may have vendor-specific automation/pre-integrated configurations to reduce manual effort.
- **Cyber V&V Tool Gaps:** Traditional cyber tools are ineffective on IEEE802.1DP networks, which only allow pre-scheduled, authorized traffic and drop all unsolicited scans by design. There are currently no cyber tools specifically designed to assess security posture within deterministic networks and a lack of tools capable of

validating traffic patterns such as verifying packet priority, measuring latency and jitter across multiple network hops, and assessing bandwidth utilization at the end-to-end application layer. The MSTC TSN Analysis Suite partially addresses these gaps by validating key functional features (e.g., traffic shaping, time synchronization, FRER) and performance metrics (e.g., latency, jitter, bandwidth). However, it currently lacks qualification, limiting its use in safety-critical environments until it is certified. A comprehensive and compliant toolset is needed to enable certification readiness under DO-178C/DO-326A for deterministic systems.

MSTC evaluates TSN devices at the Data Link Layer (Layer 2) of the Open System Interconnect (OSI) model. Future architectures, like those defined by MOSA require alignment with the Future Airborne Capability Environment (FACE) framework for software integration. To address this, MSTC will be upgraded to include FACE-compliant applications running on simulated LRUs, enabling deeper evaluation of instrumentation needs, application-level synchronization with network time, and validation of data flow through FACE applications over the TSN network. MSTC also plans to integrate an Aircraft Survivability Equipment (ASE) emulator simulate first-point integration and validate system performance, including bandwidth requirements, under operational conditions. As each Army Aviation platform will have its own future avionics architecture approach, MSTC is prepared to support component-level testing through to complete system architecture evaluation and integration.

ACKNOWLEDGEMENTS
The authors wish to acknowledge the following individuals for their contributions: Casey Carter, PeopleTec Senior Technical Fellow; Dr. David Noever, PeopleTec Chief Scientist; Jordan Parker, PeopleTec System Engineer; James Baker, Network Architect; Sam Hart, Software Engineer; and Ryan Chandler, Flight Instrumentation SME at RTC.

REFERENCES
Aeronautical Radio, Inc. (ARINC). (2009). *ARINC Specification 664: Aircraft Data Network, Part 7 (Avionics Full-Duplex Switched Ethernet)*. Annapolis, MD: ARINC.

Castro-Lara, L., Vera-Soto, P., Fortes, S., Escaño, V., Ortiz, R., & Barco, R. (2025). Deployment of a testbed for validation of TSN networks in avionics. Aerospace, 12(3), 186. https://doi.org/10.3390/aerospace12030186

Data Device Corporation. (2016). MIL-STD-1553 evolves with the times (white paper). https://www.ddc-web.com/resources/FileManager/dbi/Whitepapers/WP_1553Evolution.pdf

Tyagi, A. (2017, May 4). *The evolution and significance of AFDX in modern aircraft systems*. Logic Fruit Technologies. https://www.logic-fruit.com/blog/avionics/afdx/

Finzi, A., Mifdaoui, A., Frances, F., & Lochin, E. (2018). Network Calculus-based Timing Analysis of AFDX Networks with Strict Priority and TSN/BLS Shapers. *IEEE 13th International Symposium on Industrial Embedded Systems (SIES)*, Graz, Austria, 2018.

IEEE. (2017). IEEE standard for local and metropolitan area networks—Bridges and bridged networks—Amendment 31: Stream reservation protocol (SRP) enhancements and performance improvements (IEEE Std 802.1Qcc-2017). https://standards.ieee.org/ieee/802.1Qcc/5784/

IEEE 802.1. (2021). *Aerospace TSN use cases, traffic types, and requirements* [white paper]. https://www.ieee802.org/1/files/public/docs2021/dp-Jabbar-et-al-Aerospace-Use-Cases-0321-v06.pdf.

IEEE Standards Association & SAE International. (2025). IEEE P802.1DP/D3.0: Draft standard for local and metropolitan area networks—Time-sensitive networking for aerospace onboard Ethernet communications (SAE AS6675™-2025).

Jabbar, A. (2024, September 12). Time-sensitive networking for aerospace: Evolution of onboard networks [Conference presentation]. IEEE Standards Association Webinar Series.

Janiczek, J. (2021, July 9). Avionics data bus users demand more reliability and flexibility. Military Embedded Systems. https://militaryembedded.com/avionics/databus/avionics-databus-users-demand-more-reliability-and-flexibility

Pop, P., Craciunas, S. S., & Schedel, R. (2018). Design optimizations for time-sensitive communication in cyber-physical systems. ACM Transactions on Cyber-Physical Systems, 2(4), 1–30. https://doi.org/10.1145/3185503

Seol, Y., Hueon, D., Min, J., Kim, M., & Paek, J. (2021). Timely Survey of Time Sensitive Networking, Past and Future Directions. IEEE. https://ieeexplore.ieee.org/document/9576720